Perfect! That should have restored your original working configuration. Let's see the status.

Paste the output of `sudo systemctl status wazuh-manager` after running those commands.

Expected result: You should see `Active: active (running)` — meaning the manager is back online with your original working setup.

Once it's running:

- Your agents (Raistlin, Takhisis, etc.) will reconnect automatically.
- Suricata on Raistlin will resume sending Nmap alerts (at level 3).
- The dashboard will be accessible again.

Next step (once confirmed running):
Add the **minimal custom Nmap rule** to elevate those alerts to level 12 + MITRE T1046:

Bash

```bash
sudo bash -c 'cat > /var/ossec/etc/rules/local_rules.xml << "EOF"
<?xml version="1.0" encoding="UTF-8"?>
<group name="nmap_detection">
  <rule id="100201" level="12" overwrite="yes">
    <if_sid>86601</if_sid>
    <description>High-severity Nmap port scan detected</description>
    <mitre>
      <id>T1046</id>
    </mitre>
  </rule>
</group>
EOF'

sudo chown root:wazuh /var/ossec/etc/rules/local_rules.xml
sudo chmod 640 /var/ossec/etc/rules/local_rules.xml
sudo systemctl restart wazuh-manager
```

Then run your Nmap scan — you'll see the level 12 alerts, spike on the graph, and T1046 highlighted in MITRE.

Paste the status output now — we're back to success! 🚀